(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 April 2006 (20.04.2006)

PCT

(10) International Publication Number
WO 2006/041742 A2

(51) International Patent Classification:
G06F 12/14 (2006.01)

(21) International Application Number:
PCT/US2005/035353

(22) International Filing Date:
30 September 2005 (30.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/959,345 6 October 2004 (06.10.2004) US

(71) Applicant (*for all designated States except US*): **MACROVISION CORPORATION** [US/US]; 2830 De La Cruz Blvd., Santa Clara, CA 95050 (US).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **MOORE, James, Edward** [GB/GB]; 3 Orchard Road, Colchester, Essex CO1 1SG (GB).

(74) Agent: **SALTER, James, H.**; Macrovision Corporation, 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DEMAND BASED METHOD FOR INTERDICTION OF UNAUTHORIZED COPYING IN A DECENTRALIZED NETWORK

(57) Abstract: A multi-level and/or demand based method and apparatus for interdicting unauthorized copying in a decentralized network are described. In their preferred embodiments, the method and apparatus start out by performing search result manipulation to interdict unauthorized copying of protected files. If a trigger event is detected in network communications, however, such as a threshold number of requests being exceeded for a protected file by a network node, then the method floods that node with decoys of the protected file to enhance interdiction efforts.

WO 2006/041742 A2

DEMAND BASED METHOD FOR INTERDICTION OF UNAUTHORIZED COPYING IN A DECENTRALIZED NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part to U.S. Application Serial No. 10/803,784 filed March 18, 2004, which claims priority to U.S. Provisional Application Serial No. 60/514,429 filed October 25, 2003, U.S. Provisional Application Serial No. 60/514,430 filed October 25, 2003, U.S. Provisional Application Serial No. 60/518,691 filed November 10, 2003, and U.S. Provisional Application Serial No. 60/528,466 filed December 10, 2003.

FIELD OF THE INVENTION

[0002] The present invention generally relates to copy protection techniques and in particular, to a demand based method for interdiction of unauthorized copying in a decentralized network.

BACKGROUND OF THE INVENTION

[0003] Unauthorized copying in decentralized networks using peer-to-peer (P2P) file sharing has become a major concern to owners of copyrighted material. Unlike a centralized network, decentralization makes it commercially impractical to pursue all copyright violators in court. This is because decentralization requires filing lawsuits against virtually millions of client computer operators instead of only one party operating a central computer.

[0004] Accordingly, copyright owners seek other methods for protecting their copyrighted material, such as blocking, diverting or otherwise impairing the unauthorized distribution of their copyrighted works on a publicly accessible decentralized or P2P file trading network. In order to preserve the legitimate expectations and rights of users of such a network, however, it is desirable that copyright owners do not alter, delete, or otherwise impair the integrity of any computer file or data lawfully residing on the computer of a file trader.

OBJECTS AND SUMMARY OF THE INVENTION

[0005] Accordingly, it is an object of the present invention to provide a method and apparatus for interdiction of unauthorized copying in decentralized networks.

[0006] Another object is to provide such method and apparatus so that the legitimate rights and expectations of users of the decentralized network are preserved.

[0007] Still another object is to provide such method and apparatus such that the decentralized network is not prevented from operating for legitimate file sharing activities.

[0008] Yet another object is to provide such method and apparatus so that copies of files on the decentralized network are not destroyed through erasure or corruption of data.

[0009] These and additional objects are accomplished by the various aspects of the present invention, wherein briefly stated, one aspect is a method for interdicting unauthorized copying in a decentralized network, comprising: performing a first level of interdiction of unauthorized copying in a decentralized network having a plurality of nodes; detecting a trigger event associated with at least one of the plurality of nodes; and performing a second level of interdiction of unauthorized copying specifically directed to the at least one of the plurality of nodes.

[0010] Another aspect is a method for interdicting unauthorized copying in a decentralized network, comprising: performing a first interdiction technique for interdicting unauthorized copying in a decentralized network having a plurality of nodes; detecting a trigger event related to one of the plurality of nodes while performing the first interdiction technique; and performing a second interdiction technique directed to the one of the plurality of nodes for interdicting unauthorized copying in response to the detection of the trigger event.

[0011] Another aspect is an apparatus for interdicting unauthorized copying in a decentralized network, comprising at least one computer configured to: perform a first level of interdiction of unauthorized copying in a decentralized network having a plurality of nodes; detect a trigger event associated with at least one of the plurality of nodes; and perform a second level of interdiction of unauthorized copying specifically directed to the at least one of the plurality of nodes.

[0012] Still another aspect is an apparatus for interdicting unauthorized copying in a decentralized network, comprising at least one computer configured to: perform a first interdiction technique for interdicting unauthorized copying in a decentralized network having a plurality of nodes; detect a trigger event related to one of the plurality of nodes while performing the first interdiction technique; and perform a second interdiction technique directed to the one of the plurality of nodes for interdicting unauthorized copying in response to the detection of the trigger event.

[0013] Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiment, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] **FIG. 1** illustrates a node diagram of a non-hierarchical decentralized network.

[0015] **FIG. 2** illustrates a node diagram of a hierarchical decentralized network.

[0016] **FIG. 3** illustrates a flow diagram of a method for performing a search query in a non-hierarchical decentralized network.

[0017] **FIG. 4** illustrates a flow diagram of a method for performing a search query performed by a regular node in a hierarchical decentralized network.

[0018] **FIG. 5** illustrates a flow diagram of a method for performing a search query performed by a SuperNode in a hierarchical decentralized network.

[0019] **FIG. 6** illustrates a block diagram of a system utilizing aspects of the present invention for interdicting search queries in a decentralized network.

[0020] **FIG. 7** illustrates a flow diagram of a method for interdicting search queries through search result manipulation, utilizing aspects of the present invention.

[0021] **FIG. 8** illustrates a flow diagram of a method for quarantining a node, utilizing aspects of the present invention.

[0022] **FIGS. 9-12** illustrate nodal diagrams as an example of the method for quarantining a node, utilizing aspects of the present invention.

[0023] **FIG. 13** illustrates a flow diagram of a method for interdicting search queries through file impersonation, utilizing aspects of the present invention.

[0024] **FIG. 14** illustrates a flow diagram of a method for interdicting search queries through file transfer attenuation, utilizing aspects of the present invention.

[0025] **FIG. 15** illustrates a flow diagram of a demand based method for interdicting unauthorized copying in a decentralized network, utilizing aspects of the present invention.

[0026] **FIG. 16** illustrates a flow diagram of a preferred embodiment of a demand based method for interdicting unauthorized copying in a decentralized network, utilizing aspects of the present invention.

[0027] **FIG. 17** illustrates a block diagram of an apparatus for performing a demand based method for interdicting unauthorized copying in a decentralized network before connecting a controlled node, utilizing aspects of the present invention.

[0028] **FIG. 18** illustrates a block diagram of an apparatus for performing a demand based method for interdicting unauthorized copying in a decentralized

network after connecting a controlled node, utilizing aspects of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0029] In a decentralized network, there is no central authority or managing entity. Each node of the network makes decisions autonomously to connect, disconnect, and share information with other nodes in the network according to a predetermined protocol established by the creators of the network. Files and documents are stored in the nodes of the networks and propagated throughout the network via inter-nodal exchange. Users search the network using search queries at their respective nodes for specific files or documents and then select a host from search results to download or stream the content from.

[0030] To prevent downloading of protected files, various methods for search result manipulation and interdiction are described herein. These methods vary to some extent by the type of file sharing network that they are operating in. To illustrate the various aspects of the present invention, two networks, respectively referred to as Type A and Type B networks, are used as examples throughout the following description.

[0031] **FIG. 1** illustrates, as an example, a node diagram of a Type A, non-hierarchical decentralized network **100**. In this network structure, all nodes such as nodes N11~N19 are treated as equals. **FIG. 2**, on the other hand, illustrates, as an example, a node diagram of a Type B, hierarchical decentralized network **200**. In this second network, there are regular nodes such as nodes N20~N28, and so-called SuperNodes such as SuperNodes SN0~SN2. Regular nodes represent computers hooked to the network **200** that host or are capable of hosting files for sharing. SuperNodes are computers hooked to the network **200** that not only host or are capable of hosting files for sharing, but also have higher resources than regular nodes and generally perform functions in addition to those of regular nodes.

[0032] **FIG. 3** illustrates a flow diagram of a method for performing a file or document search in a Type A, non-hierarchical decentralized network such as the network **100**. In **301**, when a user of a node (such as node N10 in **FIG. 1**) initiates a search by generating a search (or keyword) string, the node operated by the user (hereinafter referred to as the "client node") receives and records that search string. In some systems, the name of a file that is being requested is hashed to get a key or hash value, and the key or hash value is sent out in the search string for matching.

[0033] In **302**, the client node then forwards the search string to other nodes in the decentralized network. It may do this, for example, by forwarding the search string to one or more of its neighboring nodes (i.e., nodes that it is in communication with through the decentralized network software, such as nodes N11, N12 and N13 with respect to node N10 in **FIG. 1**), which in turn, forward the search string to their neighboring nodes (such as nodes N14, N15 and N16 with respect to node N13 in **FIG. 1**), and so on, throughout the decentralized network. Note that the precise behavior of the search string handling, forwarding and query match returning process depends on the defined rules and/or policies of the decentralized network.

[0034] Each node receiving the search string checks its file list for matches, and sends information of any query matches back through the decentralized network so as to be received by the client node in **303**. Information of the query matches includes information on how to locate the file such as an URL. Hash values for each of the references (i.e., files or documents) may also be sent in the query matches. All query matches (also referred to herein as "search results") are generally sent back along the path that they came.

[0035] In **304**, all received query matches are collated and displayed on a display screen by the client node for its user. In **305**, the client node receives a selection (i.e., file or document) indicated by its user, and in **306**, it manages a P2P transfer with the selected file's host node(s). For example, the client node

may establish a direct connection with the node(s) having a copy of the selection available for download, and sends an HTTP request to those node(s) requesting the selection. The node(s) may then reply with a standard HTTP response.

[0036] **FIGS. 4-5** illustrate a flow diagram of a method for performing a search query in a Type B, hierarchical decentralized network such as the network **200**. In particular, **FIG. 4** illustrates actions taken by a client node initiating the search string (such as node N20 in **FIG. 2**), and **FIG. 5** illustrates corresponding actions taken by a SuperNode (such as SuperNode SN0 connected to node N20 in **FIG. 2**) receiving the search string.

[0037] Referring now to **FIG. 4**, in **401**, when a user of a node (such as node N20) initiates a search by generating a search (or keyword) string, the node operated by the user (i.e., the "client node") receives and records that search string. In **402**, the client node then forwards the search string to a SuperNode (such as SN0), which in turn, performs activities described in reference to **FIG. 5**. In **403**, the client node receives a prioritized list of matches back from the SuperNode and displays it on a display screen of the client node. In **404**, the client node receives a selection indicated by its user, and in **405**, it manages a P2P transfer with the selected file's host node(s) in much the same fashion as described in reference to **305** of **FIG. 3**.

[0038] Referring now to **FIG. 5**, in **501**, a SuperNode receives and records the search string from the client node. In **502**, it checks the search string against its file list, which includes files that it hosts as well as files available on other nodes connected to it (such as regular nodes N22 and N21 connected to SuperNode SN0) to generate a list of local matches. In **503**, it forwards the search string to all or a subset of SuperNodes connected to it (such as SuperNodes SN1 and SN2 connected to SuperNode SN0). These SuperNodes may in turn forward the search string to other SuperNodes connected to them, and so on, wherein the number of levels the search string is forwarded depends on the defined rules and/or policies of the decentralized network.

[0039] Each of the SuperNodes receiving the search string then checks its file list for matches, and sends information of query matches (as lists of local matches) back through the decentralized network so as to be received by the original SuperNode in **504**. In **505**, the original SuperNode (i.e., the SuperNode first receiving the search string) then generates a list of prioritized matches from all the lists of local matches (including its own). Prioritization in this case is commonly done, for example, by connection speed and quality of the file. Finally, in **506**, the prioritized list of matches is transmitted back to the client node from which the search string originated.

[0040] Additional details on decentralized networks may be found from publicly available information for decentralized peer-to-peer technologies and protocols such as Freenet, GNUtella, and Fastrack, wherein detailed knowledge of each such decentralized network is useful in implementing the various aspects of the present invention.

Interdiction System

[0041] **FIG. 6** illustrates a block diagram of a system **600** for interdicting unauthorized copying in a Decentralized Network **604**. A plurality of Software Agents SA-1 to SA-N are infiltrated into the Decentralized Network **604** masquerading as nodes by following all the traditions and policies of the Decentralized Network **604** so that they are virtually indistinguishable as infiltrators.

[0042] The Software Agents SA-1 to SA-N are implemented as software residing on one or more computers that communicate with nodes in the Decentralized Network **604** through individually assigned ports of the one or more computers. IP addresses for the ports may vary with time or in some other manner so that detection of the Software Agents SA-1 to SA-N as unauthorized masqueraders of nodes in the Decentralized Network **604** and their expulsion from the Network **604** are prevented or at least made considerably more difficult.

[0043] The Software Agents SA-1 to SA-N may uniformly infiltrate the Decentralized Network **604** by, for example, each of the Software Agents SA-1 to SA-N connecting to a corresponding node of a representative set of nodes in the Decentralized Network **604**. The representative set of nodes in this case is a subset of the Decentralized Network **604** from which characteristics of the entire Decentralized Network **604** may be statistically inferred.

[0044] General steps used by the Software Agents SA-1 to SA-N to infiltrate the Decentralized Network **604** include making Internet connections to other nodes in the Decentralized Network **604**, performing handshakes or login procedures with those other nodes as specified by the protocol of the Decentralized Network **604** in order to be recognized as nodes of the Decentralized Network **604**, and conducting searches and performing operations that regular nodes routinely do in the Decentralized Network **604** while clandestinely also performing interdiction functions.

[0045] In addition, if the Software Agents SA-1 to SA-N are to masquerade as Supernodes in the Decentralized Network **604**, they also inform the Decentralized Network **604** that they are Supernodes upon logging in and/or they are configured or at least inform the Decentralized Network **604** that they are configured to meet all of the criteria for a Supernode according to the policies of the Decentralized Network **604**.

[0046] In order to perform the above infiltration, it is useful to first identify nodes in the Decentralized Network **604** that the Software Agents SA-1 to SA-N can make Internet connections to. One way to do this is for a node controlled by the interdicting system to first join the Decentralized Network **604** as a regular client by logging in through client application software provided by or otherwise associated with the Decentralized Network **604**, receiving addresses of nodes of the Decentralized Network **604** after logging in, and storing the addresses in a node address cache for later use. The node addresses may be provided in an initial list of node addresses received upon logging in, as well as

additional node addresses resulting from connecting to one or more nodes in the initial list of nodes.

[0047] The number of the Software Agents SA-1 to SA-N, their attributes as reported to other nodes in the Decentralized Network **604**, and the geographical locations of the one or more computers upon which they reside are preferably determined by the number and geographical distribution of the nodes of the Decentralized Network **604** so that the Software Agents SA-1 to SA-N receive a desired percentage of search related communications traveling through the Decentralized Network **604**.

[0048] Each of the Software Agents SA-1 to SA-N receives search queries from client nodes requesting files in the Decentralized Network **604**, and forwards those search queries to other nodes in the Decentralized Network **604** so as to behave just like a regular node in this respect. When the Software Agents SA-1 to SA-N receive search results back from those forwarded search queries, however, rather than passing those search results back along the same path that the Software Agents SA-1 to SA-N received the corresponding search queries, they first send the search results to a Query Matcher **602** implemented as software residing on a computer connected to the Software Agents SA-1 to SA-N through a private network.

[0049] The Query Matcher **602** compares each of the references in the search results to entries in its own Database **603** containing metadata including content identification codes of protected files. Matches are then sent back to each of the Software Agents SA-1 to SA-N for search results received by the Query Matcher **602** from that Software Agent.

[0050] A Central Coordinating Authority **601** implemented as software on a computer coordinates activities of the plurality of Software Agents SA-1 to SA-N so as to interdict unauthorized copying in the Decentralized Network **604**. It does this by sending instructions to the plurality of Software Agents SA-1 to SA-N through a private network specifying actions to be taken when the plurality of

Software Agents SA-1 to SA-N receive matches of search results with protected files back from the Query Matcher **602**.

Search Result Manipulation

[0051] **FIG. 7** illustrates a flow diagram of a method for interdicting search queries through search result manipulation. In **701**, a Software Agent infiltrates a decentralized network resembling or masquerading as a node along with other Software Agents as described in reference to **FIG. 6**. The node may be any node in a non-hierarchical network, or it may be a SuperNode in a hierarchical network. In **702**, the Software Agent captures search results on their way back to a client node from which its corresponding search string originated.

[0052] In **703**, the Software Agent identifies files, documents and/or programs that it has been chartered to protect (also referred to herein cumulatively as "protected files") in the search results. For example, it may do this by sending the search results to a Query Matcher and receiving matches for protected files back from the Query Matcher as previously described in reference to **FIG. 6**.

[0053] In **704**, the Software Agent modifies the search results so as to interdict unauthorized copying of the protected files according, for example, to instructions provided to it by a Central Coordinating Authority as previously described in reference to **FIG. 6**. In **705**, the Software Agent then forwards the modified search results through the decentralized network so that it is subsequently received by the client node which originated the corresponding search string.

[0054] The Software Agent may employ any one or more of several techniques to modify the search results in **704** so as to interdict unauthorized copying in the decentralized network. In all of these techniques, however, a key feature is that none of the actual files that are residing on nodes in the decentralized network and being made available by those nodes for file sharing

are damaged in any way. The techniques only interdict unauthorized copying of protected files in the decentralized network.

[0055] One such technique to modify the search results in **704** is to simply delete all or a subset of the references that correspond to matches with protected files in the search results.

[0056] Another technique to modify the search results in **704** is to modify information for the references corresponding to matches with protected files so that they point to, for examples, an IP address that is invalid, or an IP address for a computer that does not host the requested content, or an IP address for a computer that is not even running the client application software for the decentralized network.

[0057] Another technique to modify the search results in **704** is to modify information for the references corresponding to matches with protected files so that they point to alternative files on their respective host nodes (i.e., nodes identified in the search results as having the protected files available for file sharing). Selection of the alternative files in this case may be made by random or non-random selection of non-protected files (i.e., files, documents or programs that the Software Agent is not chartered to protect).

[0058] Another technique to modify the search results in **704** is to modify information for the references corresponding to matches with protected files so that they point to one or more alternative files residing on a Controlled Node. Selection of the alternative files may be made by random or non-random selection of files on a Controlled Node, as long as the alternative files being pointed to are not protected files. The Controlled Node may be a Software Agent or another node that is controlled by the Central Coordinating Authority **601**.

[0059] Since the node is controlled in this case, there is flexibility in the form and/or content of the alternative file being pointed to. For example, the alternative file may be a synthesized decoy, or another file that is freely distributable, or a rights managed version of the protected file (i.e., one that has

added controls and/or features to make it compatible with a digital rights management system).

Synthesis of Decoy Files

[0060] Decoys are used to impersonate protected files. In particular, Decoys are files having the same properties such as filename and metadata as the files that they are impersonating, but have different content. Hash values provided by the Decoys, however, generally match their actual content, not the content of the files that they are impersonating. The following describes ways in which decoys can be algorithmically synthesized to impersonate protected audio, video, application, image and document files.

[0061] For all file types, the title of the synthesized decoy will be a random combinatorial reordering of words and phrases from the title of the protected file. The mouse over property of the file will be the same as the title.

[0062] For audio files, the content can be white noise or an anti-piracy message. The MIME type will be randomly selected from one of the commonly used types for audio (such as wave, or aiff). The length of the file is chosen at random from a range that corresponds to the size range of the known instances of the file on the Network.

[0063] For video files, the content will be snow or white noise. The MIME type will be randomly selected from one of the commonly used types for video (such as mpeg, avi, or quicktime). The length of the file is also chosen at random from a range that corresponds to the size range of the known instances of the file on the Network.

[0064] For applications, the content will be a "no operation" or NOP executable that simply terminates when executed. The type will be randomly selected from one of the commonly used types (such as ZIP).

[0065] For image files, the content will be snow or an anti-piracy statement. The MIME type will be randomly selected from one of the commonly

used types for images (such as jpg, tif, or gif). The color depth and resolution are also randomly chosen (e.g., 1600x800 resolution, 16 bit depth).

[0066] For documents, the content is blank and the MIME type is randomly selected from one of the commonly used types for documents (such as zip, pdf, doc, ppt, rtf, or html).

[0067] As just one example, the algorithmically synthesized decoy for a protected audio file for Madonna's Ray of Life track could include a title Ray of Life Track by Madonna. The content of the file, however, could be just white noise. The MIME type could be mp3 (or any of the common audio mime types) and the length of the audio file could be 3.5 minutes. Mouse over on the decoy would display the file title which would closely match the title of the protected file.

[0068] In addition to, or in lieu of, modifying the search results in **704**, the interdiction system of the present invention may also perform other activities for interdicting unauthorized copying in a decentralized network.

Nodal Quarantining

[0069] One such activity is nodal quarantining, wherein a node to be quarantined is surrounded with Software Agents by, for example, the Central Control Authority **601**. Using nodal quarantining, a node that is identified as having protected files available for file sharing can be effectively eliminated from the decentralized network by making it "invisible" to other nodes on the decentralized network or its file sharing activity restricted, but not completely eliminated, so as to interdict unauthorized copying of protected files while allowing it to share non-protected files with other nodes in the decentralized network.

[0070] **FIG. 8** illustrates a flow diagram of a method for quarantining a node, and **FIGS. 9-12** illustrate a simple step-by-step example of the method using node diagrams. In **801**, after identifying a node C to be quarantined, a list of its immediate neighbor nodes, N1 and N2, is obtained from that node (**FIG. 9**).

In **802**, a Software Agent SA1 is connected to a neighbor node N1 and the node C (**FIG. 10**). In **803**, that neighbor node N1 is then disconnected from the node C (left side of **FIG. 11**).

[0071] Depending upon the capabilities and protocol of the decentralized network, the neighbor node N1 may be disconnected using any one of numerous different techniques such as:

1) issuing a "Disconnect from node C" message to node N1, or vice versa;
2) issuing a "Disconnect from the Network" message to node N1;
3) issuing a message to node C, purporting to be from the neighbor node N1, indicating that node N1 is now disconnecting, or vice versa;
4) issuing a message to node N1 that violates the agreed upon connection protocol between node N1 and node C, thus inducing node N1 to abandon the connection, or vice versa;
5) attaching a very large number of Software Agents to node C so that its capacity or quota of immediate neighbors is exceeded, thus inducing node C to disconnect from one or more of its immediate neighbor nodes until node N1 is disconnected;
6) attaching a very large number of Software Agents to node C so that its capacity or quota of immediate neighbors is exceeded, thus inducing node C to transfer connections for one or more of its immediate neighbor nodes to a single neighbor node until node N1 is disconnected from node C;
7) overwhelming the capacity of node C's port, socket or connection to node N1 by bombarding it with messages or requests that it must parse, act upon, or otherwise process; or
8) eliminating or disconnecting N1 from the decentralized network altogether by exploiting a known defect in the client software

application for the decentralized network or underlying client operating system running on the node N1 (e.g., overrun the stack).

[0072] It is noted with regards to this last disconnect technique that documentation of such bugs is available in the public domain, albeit ephemerally, for most software clients of popular, large-scale distributed networks.

[0073] In **804**, the method determines whether there is a neighbor node that is still directly connected to the node to be quarantined. In this example, the answer is YES, so the method loops back to **802**, and another Software Agent SA2 is connected to a neighbor node N2 and the node C (right side of **FIG. 11**). In **803**, the neighbor node N2 is then disconnected from the node to be quarantined (**FIG. 12**). Then again in **804**, the method determines whether there is another neighbor node connected to the node to be quarantined. This time, however, the answer is NO, so the method terminates.

File Impersonation

[0074] Another activity for interdicting unauthorized copying in a decentralized network is file impersonation. For example, **FIG. 13** illustrates a flow diagram of a method for interdicting unauthorized copying in a decentralized network through file impersonation. In **1301**, a Software Agent infiltrates a decentralized network resembling or masquerading as a node along with other Software Agents as described in reference to **FIG. 6**. The node in this case may be any type of node in either a non-hierarchical or hierarchical decentralized network. In **1302**, the Software Agent receives a search string just like other nodes in the decentralized network, and in **1303**, it reports matches for protected files satisfying the search string along with attributes that would qualify it as a top choice or source for the matches in the decentralized network.

[0075] In **1304**, the Software Agent receives a request for one of the reported matches, and in **1305**, it sends an alternative file instead of the actually requested file. The alternative file in this case may be a synthesized decoy file, or

a spoof file, or a file that is freely distributable, or a rights-managed version of the matched protected file.

File Transfer Attenuation

[0076] Another activity for interdicting unauthorized copying in a decentralized network is file transfer attenuation. For example, **FIG. 14** illustrates a flow diagram of a method for interdicting unauthorized copying in a decentralized network through file transfer attenuation, wherein **1401~1404** are performed in the same manner as described in reference to **1301~1304**. In **1405**, however, in addition to transmitting an alternative file, the method attenuates the transmission so that its transmission rate starts off fast, then as the download goes on, the transmission rate slows down. By the time the transmission rate slows down a lot, the user of the client node requesting the file has got most of the file so he or she will be reluctant to cancel the download at that point. Eventually, however, the transmission rate will slow down to such a trickle that the user will probably become extremely unhappy with the download progress and consequently, cancel it at that point. In this case, the download will not time out so the user must explicitly cancel it in order to terminate the transmission. Alternatively, the transmission may be automatically terminated after a certain percentage such as 95% of the file has been transmitted.

[0077] Another technique for interdicting unauthorized copying in a decentralized network is hash spoofing. Although discussed separately here, forms of hash spoofing can also be used in the search results modification method described in reference to **FIG. 7** as well as the file impersonation method described in reference to **FIG. 13**.

Hash Spoofing

[0078] In most decentralized peer-to-peer file sharing networks, whether hierarchical or non-hierarchical, each unique file is given an identification code to uniquely identify its content. Commonly, this code is a hash value generated through a cryptographic hash algorithm (such as MD-4, MD-5, SHA-1, SHA-64,

etc.) of all or a subset of the file's content. This hash mechanism is used by some decentralized networks to facilitate resuming downloads which have been interrupted for some reason before completion, or for multi-source downloading which can be used to greatly improve the reliability and speed of file downloads.

[0079] A client node sends out a search string on a decentralized network, and gets search results back along with their hashes. The file that the user of the client node wishes to download, may reside on more than one node in the decentralized network as evidenced by identical hashes. If the client node has its download interrupted for some reason, it may resume its download at a later time by finding another node having the file as identified by an identical hash value, and downloading the rest of the file at that time from that node. In addition, if the client node wants to download a file with many sources on the decentralized network and it knows that all of these sources have exactly the same content (as evidenced by their same hash values), the client node can split the file content into segments and request a few segments from each of the sources.

[0080] Once the downloads are completed, the client node then can verify that the hash given to it in the search results is identical to the hash calculated using the file content that was downloaded. If the two match, then downloading was successful. On the other hand, if they do not match, then the downloaded file is said to be corrupt, and the client node will either automatically delete it or flag it as corrupt and ask the user what to do with it.

[0081] Hash spoofing can be used for interdicting unauthorized copying where such interruption/resumption and multi-source downloading is being used in a decentralized network. In the interdiction method described in reference to **FIG. 7**, the Software Agent may modify the search results so as to replace a link to (or address of) a file to be protected with either a link to a non-existent file along with a reported hash value that doesn't correspond to any file in the decentralized network, or a link to a spoof file along with a reported hash value matching that of the file whose link is being replaced. In the first case, the client

node will try to find the non-existent file, but will be unsuccessful, because the file doesn't exist. The client node may also try to find other files with the same hash value as the non-existent file for download, but will never be able to since there are no files in the decentralized network that correspond to the hash value.

[0082] In the second case, when the Software Agent receives a request for a protected file, or a segment of the protected file in the case of a multi-source download, the spoof file or a portion thereof is transmitted instead of the requested file or segment of the file. After the client node has completed downloading the file, or all segments from its sources in the case of multi-source downloading, the hash will be calculated and a mismatch will be detected at that time (i.e., the file will be corrupted), because the hash value of the spoof file or segment thereof is different than that reported.

Multi-Level and/or Demand Based Interdiction

[0083] Although it is possible to perform all of the interdiction methods described herein simultaneously for maximum effect, such an approach may be an inefficient use of system resources as well as commercially impractical from a cost/benefit perspective. Further, some interdiction methods may be most advantageous under certain situations, while other interdiction methods are most advantageous in others.

[0084] For example, one commonly used interdiction approach is to flood a decentralized network with decoys of a protected file. This approach may be very effective when there is a large demand for the protected file. However, it can also be wasteful of system resources when the demand for the protected file is small, since a large number of controlled nodes offering the decoys for downloading in the decentralized network must be provided in order to effectively flood the network with decoys, making this approach not easily scaleable.

[0085] Conversely, some of the interdiction approaches described herein, such as search result manipulation, are readily scaleable, and therefore, are very

cost effective even when demand for a protected file is small. These approaches are especially useful for protecting large catalogues of protected files where demand for individual files may vary considerably from one to another in the catalogue. Thus, a multi-level and/or demand based approach of using one or more interdiction techniques under certain circumstances, and other interdiction techniques under other circumstances can be readily appreciated for its usefulness in cost effectively interdicting unauthorized copying of protected files in a decentralized network.

[0086] **FIG. 15** illustrates, as an example, a general approach to a multi-level and/or demand based method for interdicting unauthorized copying in a decentralized network. In **1501**, a first level of interdiction is performed to interdict unauthorized copying of protected files in a decentralized network. In **1502**, a trigger event is detected while performing the first level of interdiction. The trigger event may be related to a number of search results being sent back to one of the decentralized network nodes indicating a file that is to be protected through the first level of interdiction, or a number of search queries originating from the node indicating a file that is to be protected through the first level of interdiction. In **1503**, a second level of interdiction is performed in response to the detection of the trigger event. The second level of interdiction may include tasks performed in addition to those of the first level of interdiction, or tasks performed in lieu of those performed in the first level of interdiction. Although only two levels of interdiction are shown in this particular example, it is to be appreciated that additional levels of interdiction could be added with each additional level being triggered by a different trigger event.

[0087] **FIG. 16** illustrates, as an example, a particular and preferred multi-level and/or demand based method for interdicting unauthorized copying in a decentralized network. In **1601**, a Filterer module is run along with or as a part of a software agent masquerading as a node in the decentralized network so as to perform search result manipulation such as described in reference to **FIG. 7**.

[0088] In **1602**, a trigger event is detected by the software agent while performing the search result manipulation. The trigger event in this case is related to a number of times a protected file is referenced in search results being transmitted back to one of the nodes of the decentralized network. More particularly, the trigger event is detected when that number exceeds a threshold number programmed into or provided to the software agent.

[0089] In **1603**, a Flooder module included with or in the software agent is activated that causes the node identified in **1602** to be flooded with decoys of the protected file. Note that this is a selective flooding directed to a specific node of the decentralized network, as opposed to conventional flooding that is directed to the entire decentralized network. Because it is a selective or targeted flooding, as opposed to a shotgun flooding, it is to be appreciated that it is a far more efficient interdiction approach with respect to the utilization of system resources.

[0090] **FIGS. 17** and **18** illustrate, as an example, the operation of **1601~1603** in a hierarchical decentralized network. Referring first to **FIG. 17**, a Software Agent "SNF" performs the task of a filterer such as described in reference to **1601**, while masquerading as a SuperNode in the decentralized network so as to intercept communications within the decentralized network related to search queries.

[0091] During the performance of its interdiction tasks, the Software Agent "SNF" identifies references to protected files in the communications by interacting with a Query Matcher **602** as described in reference to **FIG. 6**. When the number of times that a reference to one of the protected files exceeds a threshold number for one of the other SuperNodes in the decentralized network, a trigger event is detected by the Software Agent "SNF". In the present example, it is assumed that SuperNode "SN1" has been identified as being associated with the trigger event.

[0092] Referring now to **FIG. 18**, in response to the detection of the trigger event, a Flooder module included with or in the Software Agent "SNF" is

activated. The Flooder module floods the identified SuperNode "SN1" with decoys of the protected file by, for example, connecting one or more controlled nodes, such as Controlled Node "CN4", as regular nodes to the SuperNode "SN1", wherein each of the controlled nodes has one or more decoys of the protected file available for downloading. Note that these nodes are referred to as controlled nodes since they are controlled by or under common control as the Software Agent "SNF".

[0093] By continuously looping through and applying **1601~1603**, the Software Agent "SNF" can selectively flood any SuperNode in the decentralized network with decoys of any protected file in a catalog of protected files after a trigger event has identified that SuperNode and that protected file as needing the additional protection afforded by such selective flooding. Although not shown in the figures, a reverse procedure may also be used wherein selective flooding is stopped when the trigger event is no longer being triggered (i.e., when the number of times that a reference identifying the protected file and included in communications associated with a given SuperNode falls below the threshold number).

[0094] Still other techniques for interdicting unauthorized copying in a decentralized network using the plurality of Software Agents, Central Coordinating Authority, and Query Matcher as described herein can also be readily conceived and are fully contemplated to be within the full scope of the present invention.

[0095] Although the various aspects of the present invention have been described with respect to a preferred embodiment, it will be understood that the invention is entitled to full protection within the full scope of the appended claims.

CLAIMS

I claim:

1. A method for interdicting unauthorized copying in a decentralized network, comprising:

performing a first level of interdiction of unauthorized copying in a decentralized network having a plurality of nodes;

detecting a trigger event associated with at least one of the plurality of nodes; and

performing a second level of interdiction of unauthorized copying specifically directed to the at least one of the plurality of nodes.

2. The method according to claim 1, wherein the trigger event is related to a number of search results being sent back to the at least one of the plurality of nodes indicating a file to be protected through the first level of interdiction.

3. The method according to claim 1, wherein the trigger event is related to a number of search queries originating from the at least one of the plurality of nodes indicating a file to be protected through the first level of interdiction.

4. The method according to claim 1, wherein the second level of interdiction includes tasks performed in addition to those of the first level of interdiction.

5. The method according to claim 1, wherein the performance of the first level of interdiction comprises:

infiltrating the decentralized network with at least one software agent masquerading as a node so as to intercept communications within the decentralized network related to search queries;

identifying references to a protected file in the communications; and

interdicting unauthorized copying of the protected file in response to the communications including such identified references of the protected file.

6. The method according to claim 5, wherein the trigger event is related to a number of the communications including such identified references of the protected file and involving the at least one of the plurality of nodes.

7. The method according to claim 6, wherein the trigger event is detected when the number of the communications including such identified references of the protected file and involving the at least one of the plurality of nodes reaches a threshold number.

8. The method according to claim 6, wherein the performance of the second level of interdiction comprises: providing decoys of the protected file to the at least one of the plurality of nodes so as to satisfy at least a majority of the communications including such identified references of the protected file and involving the at least one of the plurality of nodes.

9. The method according to claim 6, wherein the performance of the second level of interdiction comprises: flooding the at least one of the plurality of nodes with decoys of the protected file.

10. The method according to claim 5, wherein the decentralized network is an hierarchical decentralized network, the at least one

software agent masquerades as a supernode, the at least one of the plurality of nodes are other supernodes, and the performance of the second level of interdiction comprises: connecting at least one controlled node having decoys of the protected file to at least one of the other supernodes.

11. A method for interdicting unauthorized copying in a decentralized network, comprising:

performing a first interdiction technique for interdicting unauthorized copying in a decentralized network having a plurality of nodes;

detecting a trigger event related to one of the plurality of nodes while performing the first interdiction technique; and

performing a second interdiction technique directed to the one of the plurality of nodes for interdicting unauthorized copying in response to the detection of the trigger event.

12. The method according to claim 11, wherein the first interdiction technique includes search result manipulation.

13. The method according to claim 12, wherein the trigger event is related to a number of times a protected file is referenced in search results being transmitted back to the one of the plurality of nodes.

14. The method according to claim 13, wherein the second interdiction technique includes flooding the at least one of the plurality of nodes with decoys of the protected file.

15. The method according to claim 13, wherein the decentralized network is a hierarchical decentralized network, the one of the plurality of nodes is a supernode, and the second interdiction technique includes

connecting at least one controlled node having decoys of the protected file to the supernode.

16. The method according to claim 12, wherein the trigger event is related to a number of times a protected file is referenced in search queries being received from one of the plurality of nodes.

17. The method according to claim 16, wherein the second interdiction technique includes flooding the at least one of the plurality of nodes with decoys of the protected file.

18. The method according to claim 16, wherein the decentralized network is a hierarchical decentralized network, the one of the plurality of nodes is a supernode, and the second interdiction technique includes connecting at least one controlled node having decoys of the protected file to the supernode.

19. An apparatus for interdicting unauthorized copying in a decentralized network, comprising at least one computer configured to:

perform a first level of interdiction of unauthorized copying in a decentralized network having a plurality of nodes;

detect a trigger event associated with at least one of the plurality of nodes; and

perform a second level of interdiction of unauthorized copying specifically directed to the at least one of the plurality of nodes.

20. The apparatus according to claim 19, wherein the trigger event is related to a number of search results being sent back to the at least one of

the plurality of nodes indicating a file to be protected through the first level of interdiction.

21. The apparatus according to claim 19, wherein the trigger event is related to a number of search queries originating from the at least one of the plurality of nodes indicating a file to be protected through the first level of interdiction.

22. The apparatus according to claim 19, wherein the second level of interdiction includes tasks performed in addition to those of the first level of interdiction.

23. The apparatus according to claim 19, wherein the performance of the first level of interdiction comprises:

infiltrating the decentralized network with at least one software agent masquerading as a node so as to intercept communications within the decentralized network related to search queries;

identifying references to a protected file in the communications; and

interdicting unauthorized copying of the protected file in response to the communications including such identified references of the protected file.

24. The apparatus according to claim 23, wherein the trigger event is related to a number of the communications including such identified references of the protected file and involving the at least one of the plurality of nodes.

25. The apparatus according to claim 24, wherein the trigger event is detected when the number of the communications including such

identified references of the protected file and involving the at least one of the plurality of nodes reaches a threshold number.

26. The apparatus according to claim 24, wherein the performance of the second level of interdiction comprises: causing decoys of the protected file to be provided to the at least one of the plurality of nodes so as to satisfy at least a majority of the communications including such identified references of the protected file and involving the at least one of the plurality of nodes.

27. The apparatus according to claim 24, wherein the performance of the second level of interdiction comprises: causing the at least one of the plurality of nodes to be flooded with decoys of the protected file.

28. The apparatus according to claim 23, wherein the decentralized network is an hierarchical decentralized network, the at least one software agent masquerades as a supernode, the at least one of the plurality of nodes are other supernodes, and the performance of the second level of interdiction comprises: connecting at least one controlled node having decoys of the protected file to at least one of the other supernodes.

29. An apparatus for interdicting unauthorized copying in a decentralized network, comprising at least one computer configured to:

perform a first interdiction technique for interdicting unauthorized copying in a decentralized network having a plurality of nodes;

detect a trigger event related to one of the plurality of nodes while performing the first interdiction technique; and

perform a second interdiction technique directed to the one of the plurality of nodes for interdicting unauthorized copying in response to the detection of the trigger event.

30. The apparatus according to claim 29, wherein the first interdiction technique includes search result manipulation.

31. The apparatus according to claim 30, wherein the trigger event is related to a number of times a protected file is referenced in search results being transmitted back to the one of the plurality of nodes.

32. The apparatus according to claim 31, wherein the second interdiction technique includes causing the at least one of the plurality of nodes to be flooded with decoys of the protected file.

33. The apparatus according to claim 31, wherein the decentralized network is a hierarchical decentralized network, the one of the plurality of nodes is a supernode, and the second interdiction technique includes connecting at least one controlled node having decoys of the protected file to the supernode.

34. The apparatus according to claim 30, wherein the trigger event is related to a number of times a protected file is referenced in search queries being received from one of the plurality of nodes.

35. The apparatus according to claim 34, wherein the second interdiction technique includes causing the at least one of the plurality of nodes to be flooded with decoys of the protected file.

36. The apparatus according to claim 35, wherein the decentralized network is a hierarchical decentralized network, the one of the plurality of nodes is a supernode, and the second interdiction technique includes connecting at least one controlled node having decoys of the protected file to the supernode.

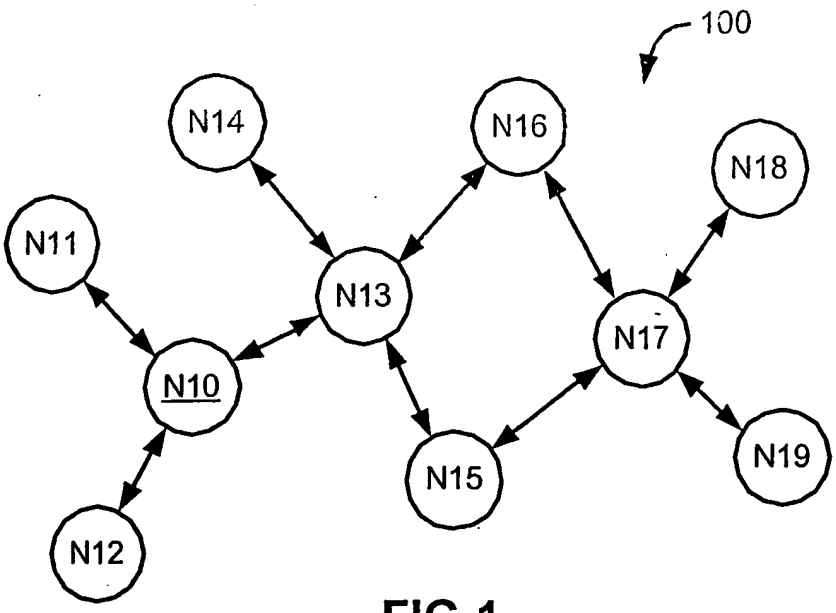

FIG.1
PRIOR ART

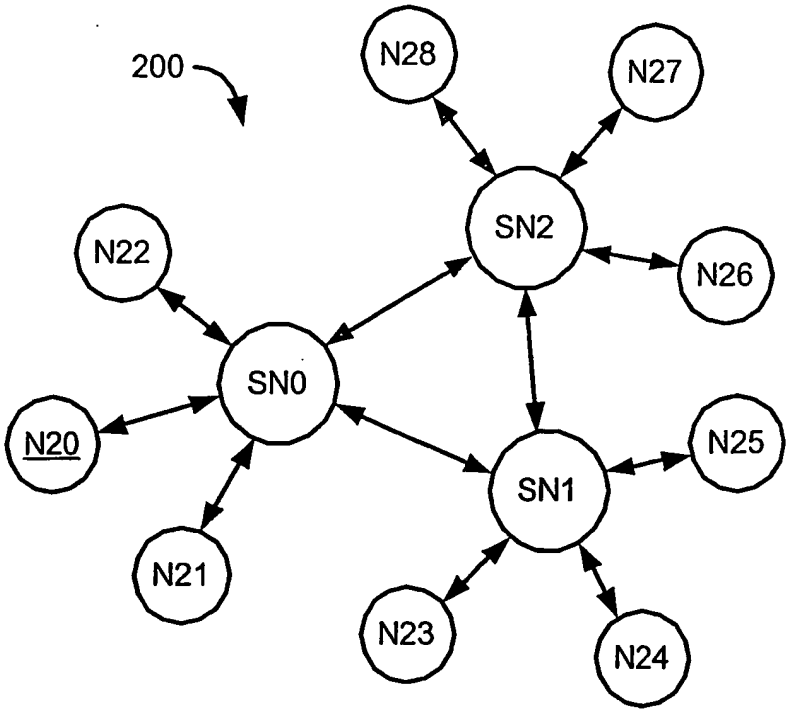

FIG.2
PRIOR ART

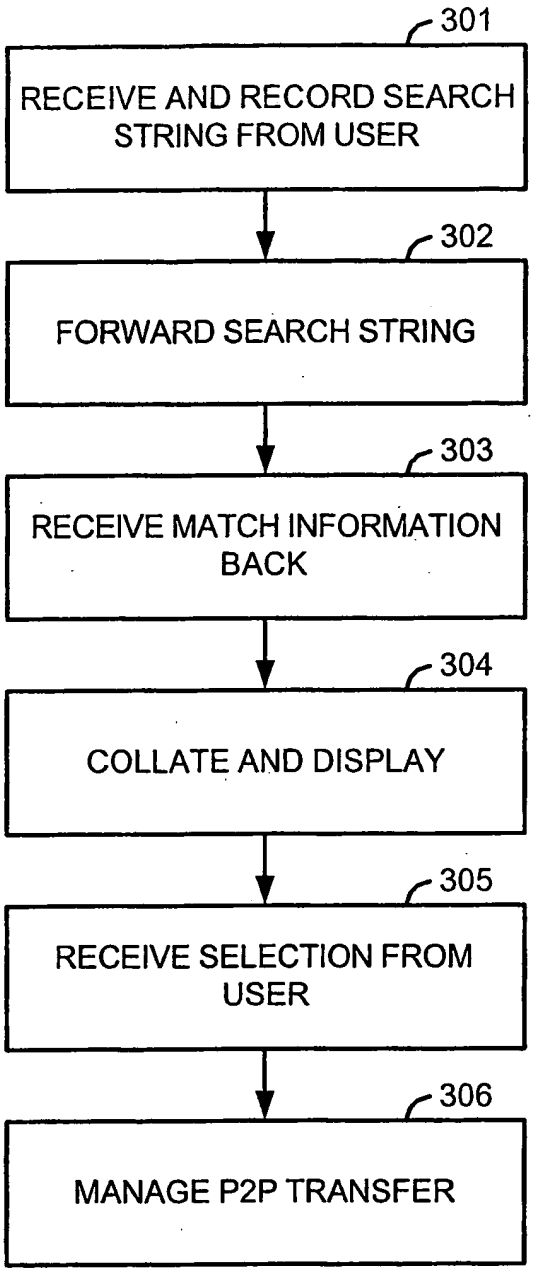

FIG.3
PRIOR ART

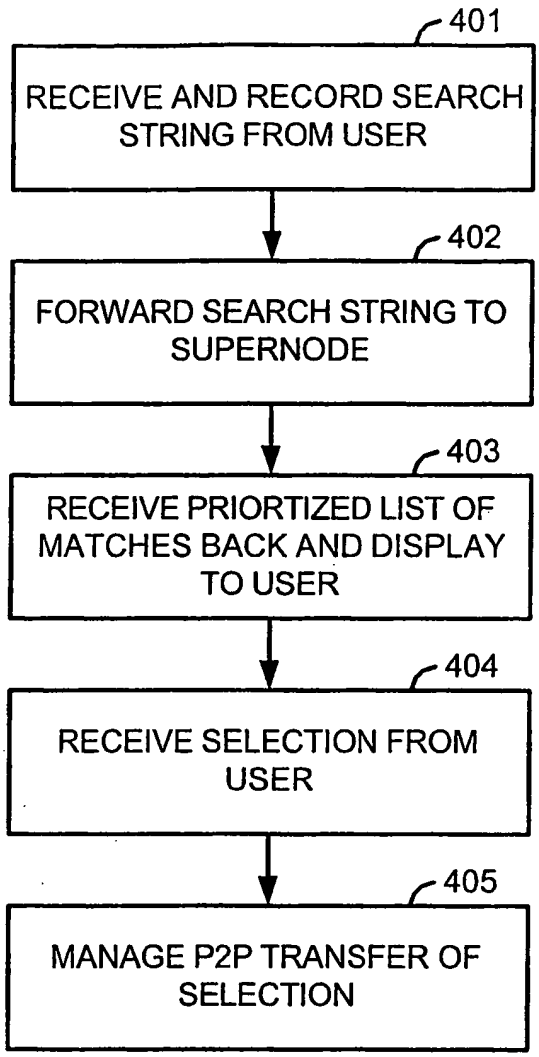

FIG.4
PRIOR ART

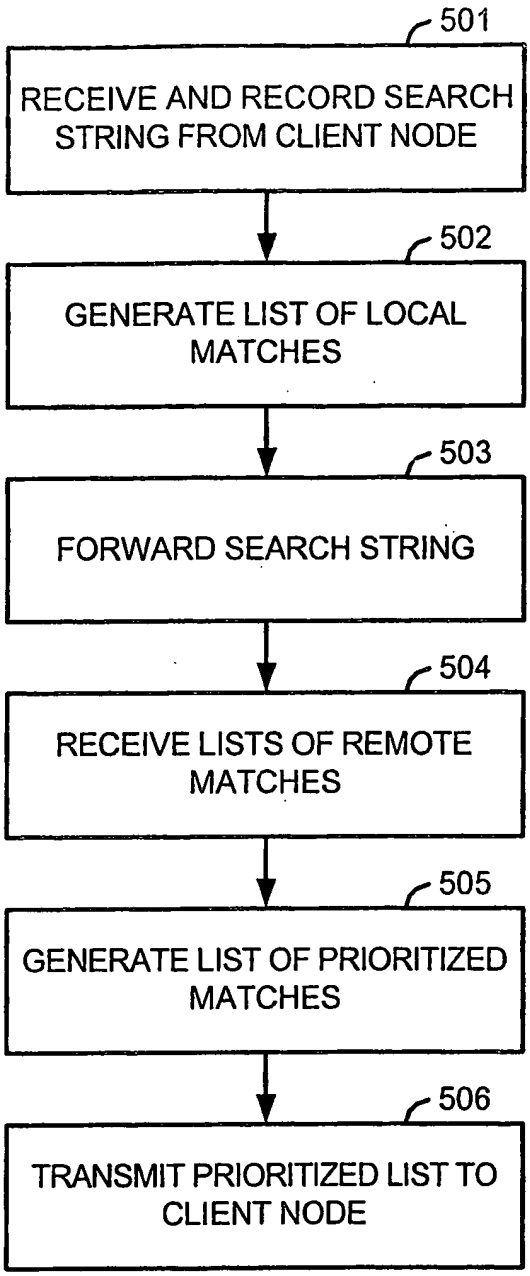

FIG.5
PRIOR ART

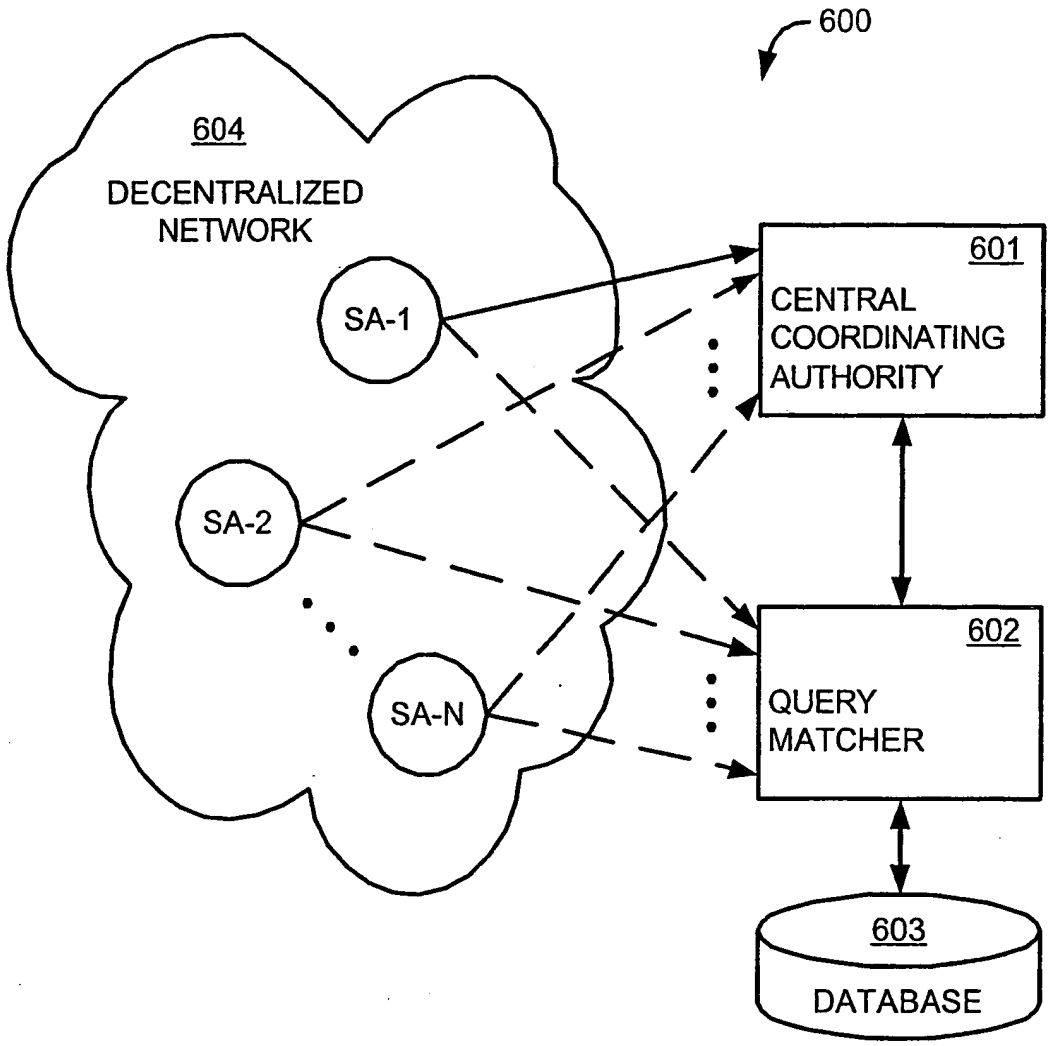
600
604
DECENTRALIZED NETWORK
SA-1
SA-2
SA-N
601
CENTRAL COORDINATING AUTHORITY
602
QUERY MATCHER
603
DATABASE

FIG.6

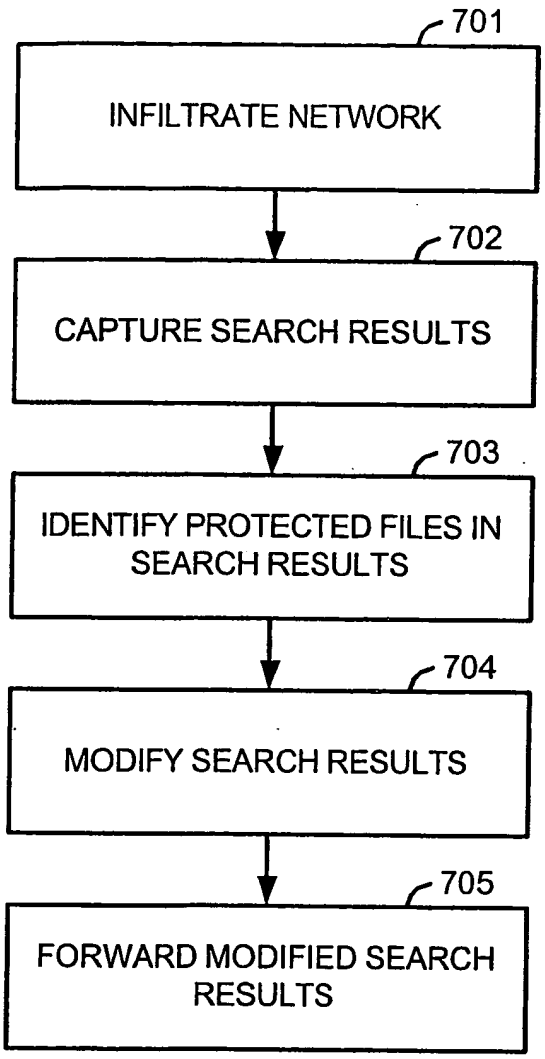
701
INFILTRATE NETWORK
702
CAPTURE SEARCH RESULTS
703
IDENTIFY PROTECTED FILES IN SEARCH RESULTS
704
MODIFY SEARCH RESULTS
705
FORWARD MODIFIED SEARCH RESULTS

FIG.7

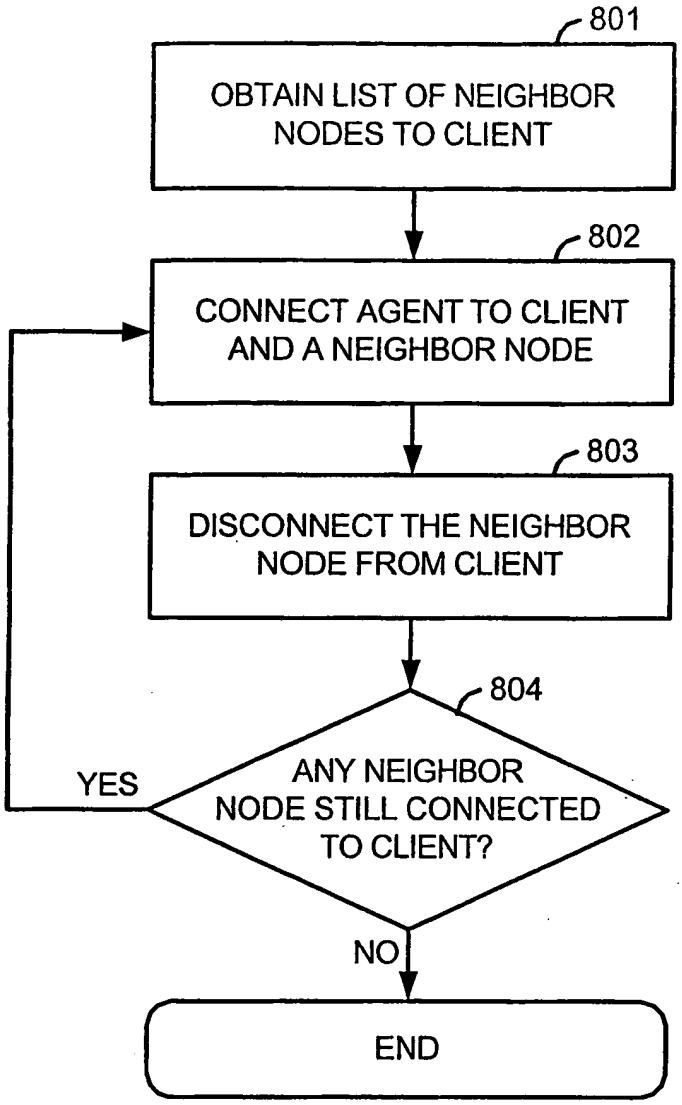
801
OBTAIN LIST OF NEIGHBOR NODES TO CLIENT
802
CONNECT AGENT TO CLIENT AND A NEIGHBOR NODE
803
DISCONNECT THE NEIGHBOR NODE FROM CLIENT
804
ANY NEIGHBOR NODE STILL CONNECTED TO CLIENT?
YES
NO
END

FIG.8

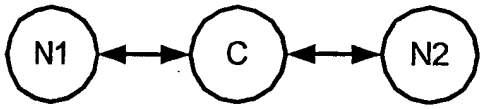

FIG.9

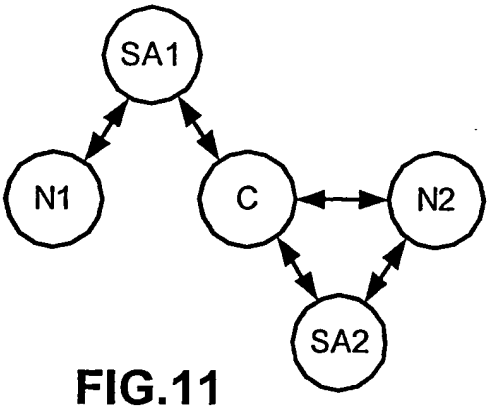

FIG.11

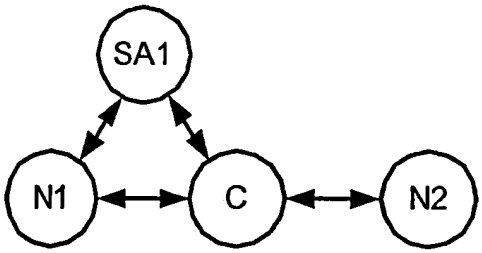

FIG.10

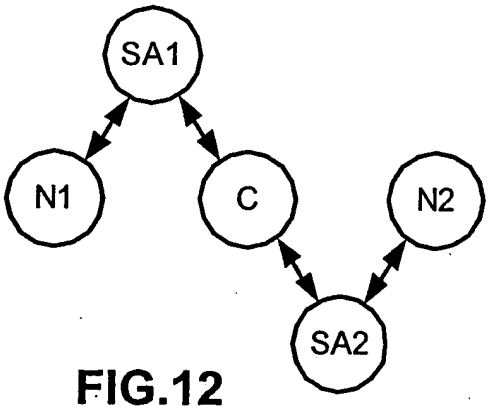

FIG.12

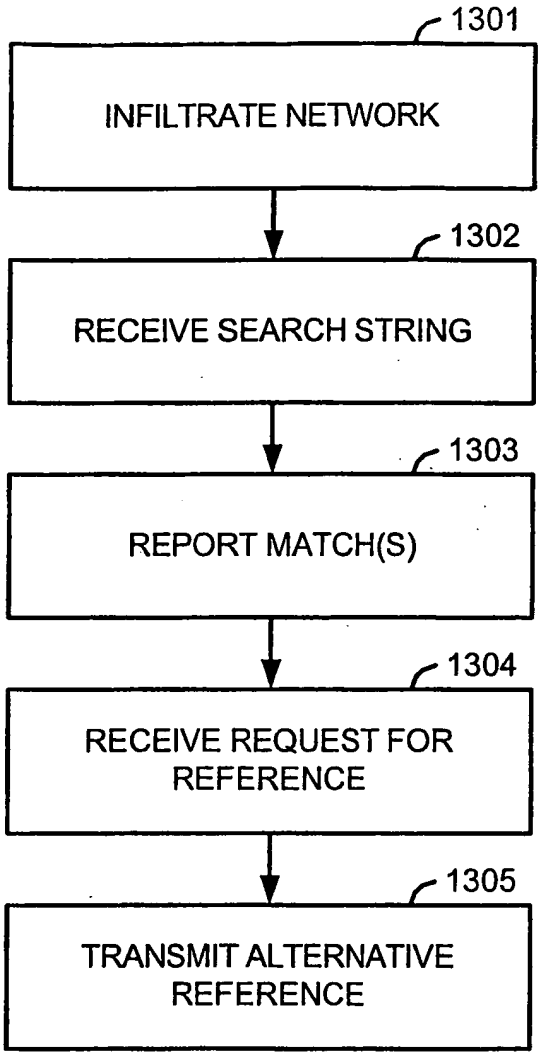
1301
INFILTRATE NETWORK
1302
RECEIVE SEARCH STRING
1303
REPORT MATCH(S)
1304
RECEIVE REQUEST FOR REFERENCE
1305
TRANSMIT ALTERNATIVE REFERENCE

FIG.13

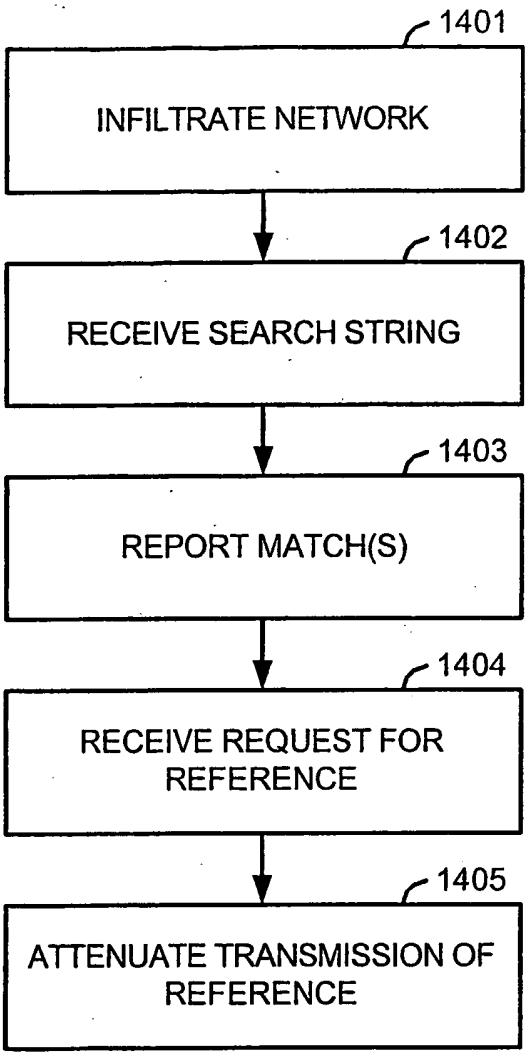
1401
INFILTRATE NETWORK
1402
RECEIVE SEARCH STRING
1403
REPORT MATCH(S)
1404
RECEIVE REQUEST FOR REFERENCE
1405
ATTENUATE TRANSMISSION OF REFERENCE

FIG.14

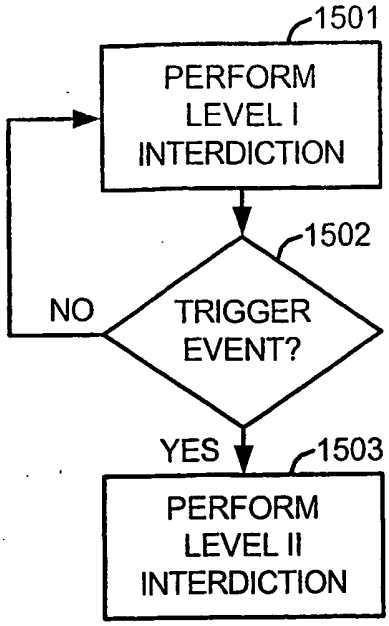
1501
PERFORM LEVEL I INTERDICTION
1502
TRIGGER EVENT?
NO
YES
1503
PERFORM LEVEL II INTERDICTION

FIG.15

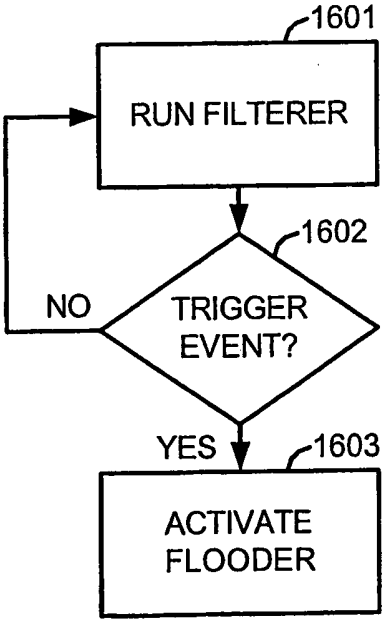
1601
RUN FILTERER
1602
TRIGGER EVENT?
NO
YES
1603
ACTIVATE FLOODER

FIG.16

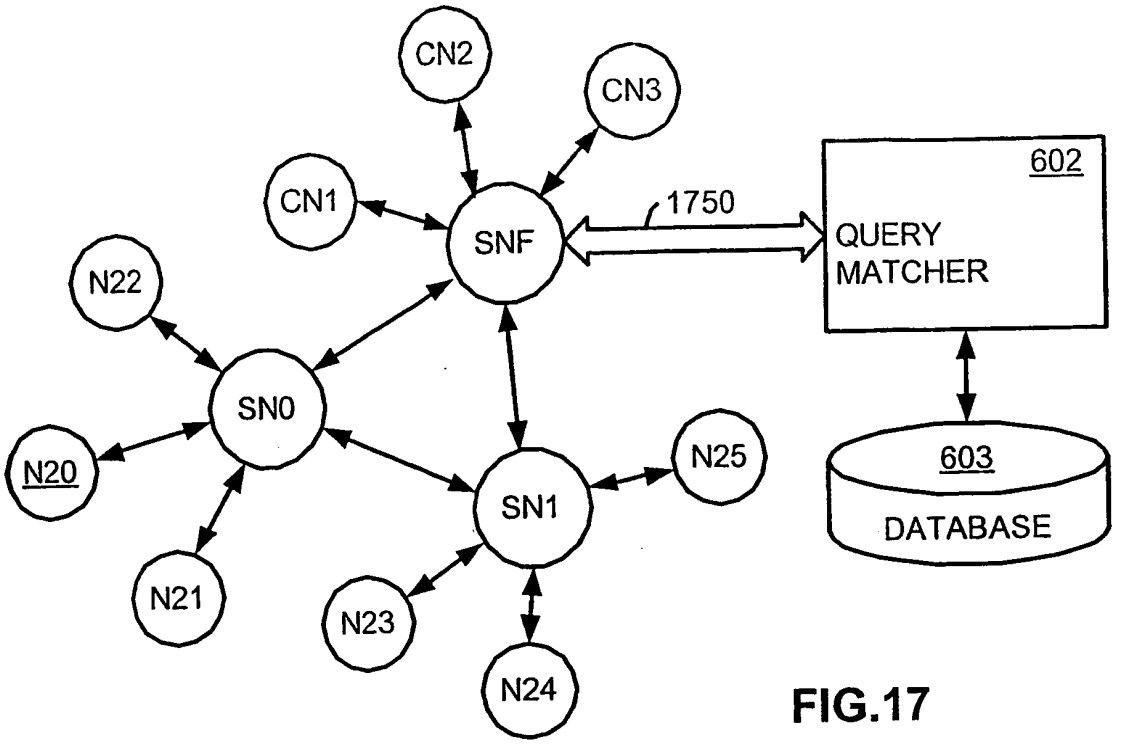
CN2
CN3
CN1
SNF
1750
602
QUERY MATCHER
N22
SN0
N20
N25
SN1
603
DATABASE
N21
N23
N24

FIG.17

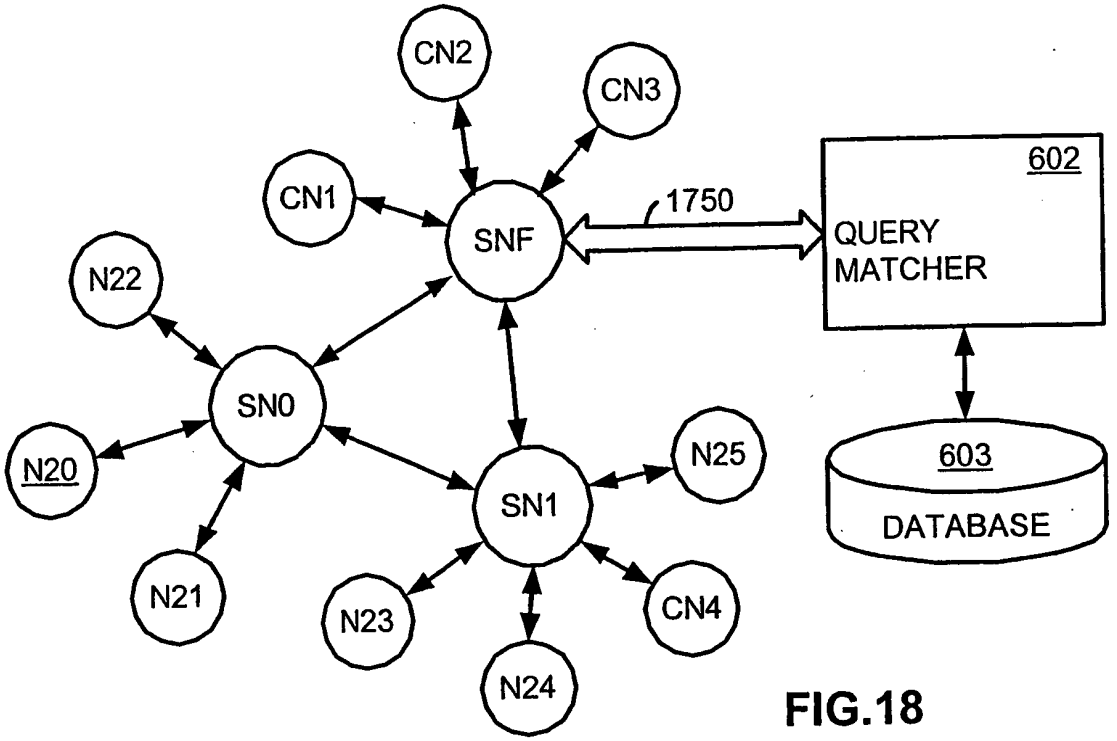
CN2
CN3
CN1
SNF
1750
602
QUERY MATCHER
N22
SN0
N20
N25
SN1
603
DATABASE
N21
N23
CN4
N24

FIG.18